NITOTV IN ASSOCIATION WITH GUARDIAN PRESENTS

CHECKRA1N 4 TVOS

#OBTS

INTRODUCTION - WHO IS THIS GUY?

KEVIN BRADLEY AKA NITOTV

- GIT major (no not THAT git) turned developer / reverse engineer
- Started hacking AppleTV's around 2008 in #awkwardtv on irc.moofspeak.net
- Joined chronic dev in 2010 when AppleTV 2 was introduced
- iOS developer at Guardian
- Run nitoTV tvOS App store with fellow cdev/sudoer @jaywalker
- Many projects in the works prior to release of Checkm8

BACKGROUND

PROJECTS BEFORE CHECKM8 IS RELEASED

SEPTEMBER 2018

- While working on nitoTV store (App Store for tvOS), decided I needed something exciting to launch with it.
- Start working on 'untitled controller project' (becomes nControl)
  - Aiming to be a native version of 'controllers 4 all'
  - PS4 / Xbox One controller support targeted for modern jailbreaks
  - Investigate updating BTStack but realize BTStack breaks Siri Remote

MARCH 2019

- 3.15.19 nControl tvOS soft release / iOS full release
    - Essentially native / revamped controllers 4 all
    - PS4/Xbox One support+ for tvOS, iOS, macOS
    - Supports a variety of other wireless & wired controllers
    - more info at wiki.awkwardtv.org/wiki/NControl
- 3.25.19 Apple announces Apple Arcade and sherlocks nControl
- Devastated, felt my store's launch would be underwhelming

BACKGROUND

JULY 2019

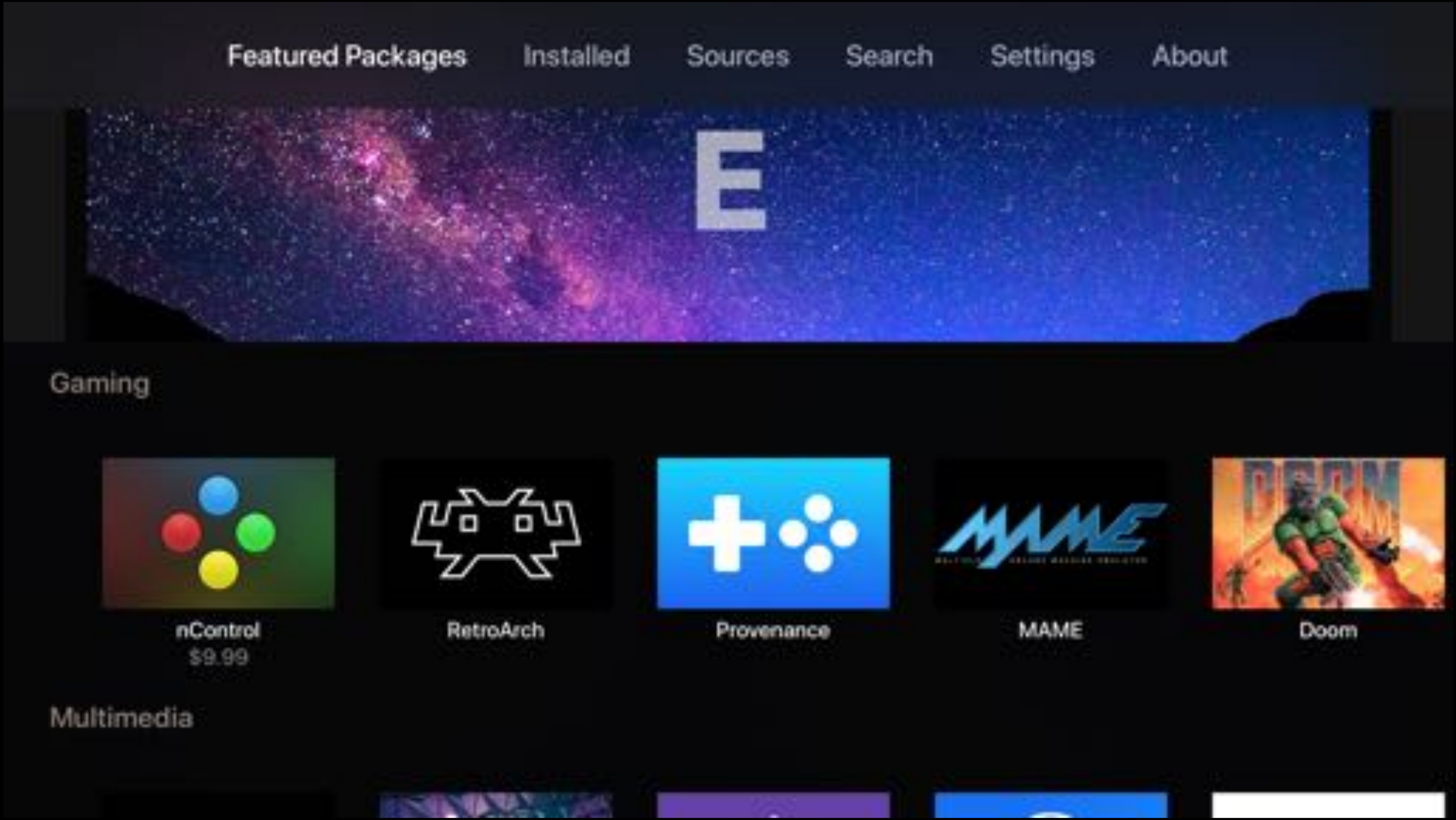
- Looking for ways to impress with nControl again....
- Start implementing MFI support into PUBG in PUBC
- PUBC is insanely popular, adapt other games.
- Mobile Legends, FIFA & Pro Evolution Soccer 2019 covered

AUGUST 2019

nito.tv store launches, first ever tvOS jailbreak App Store

Introductory blog post available here:

https://sciencography.tumblr.com/post/187244563802/growup


Featured Packages
Installed
Sources
Search
Settings
About
E
Gaming
nControl
$9.99
RetroArch
Provenance
MAME
Doom
Multimedia

NITO.TV STORE

- nControl only product (for now)
- Requires Amazon initially
- PayPal support is now live!
- Will support other developers selling products very soon

nControl

Kevin Bradley & Luca Todesco
Multimedia

Use Sony Dual Shock 4 / Slim, XBox One(S), Evo VR Pro, ipega I9400, 8bitdo *30, and Nintendo Switch Joy-Con / Pro controllers in any application that supports MFI controllers. Including em... MORE

Screenshots

CHECKM8 RELEASED

LATE SEPTEMBER

- September 27th, 2019 checkm8/ipwndfu released by @axi0mX
- There has not been an exploit like this in 10 years (limera1n, SHAtter)
- Permanent unpatchable bootrom exploit for hundreds of millions of *OS devices
- Allows dumping SecureROM, decrypting keybags for iOS firmware, and demoting device for JTAG
- AppleTV 3-5 covered for life, however, not all initially supported by checkm8 / ipwndfu
- SoC support: s5l8947x, s5l8950x, s5l8955x, s5l8960x, t8002, t8004, t8010, t8011, t8015

CHECKM8 RELEASED

LATE SEPTEMBER

- While iOS community buzzing about SecureROM exploit
- Happen to Discover 'hidden' AirDrop implementation in tvOS
- Released Breezy + Ethereal (partial AirDrop support)
- Updating chimera & electra to catch up to speed w/ iOS versions

AirDrop

nitoMBP
Bedroom
atv11

AirDrop lets you share instantly with devices nearby.
To send, turn on AirDrop on iOS or on your Mac and make the device discoverable to everyone.

Done

CHECKRA1N DEVELOPMENT

OCTOBER 2019

- iOS Jailbreak using checkm8 is in the works.
- @qwerty, @axi0mX et al start the project
- mainly debugging in early stages
- debugging on tvOS 13 was challenging

**argp, axi0mx,
danyl931, jaywalker,
kirb, littlelailo,
nitoTV,
never_released,
nullpixel, pimskeks,
qwertyoruiop,
sbingner, siguza**

EARLY DEBUGGING – SERIOUSLY...

TVOS CHALLENGE ACCEPTED

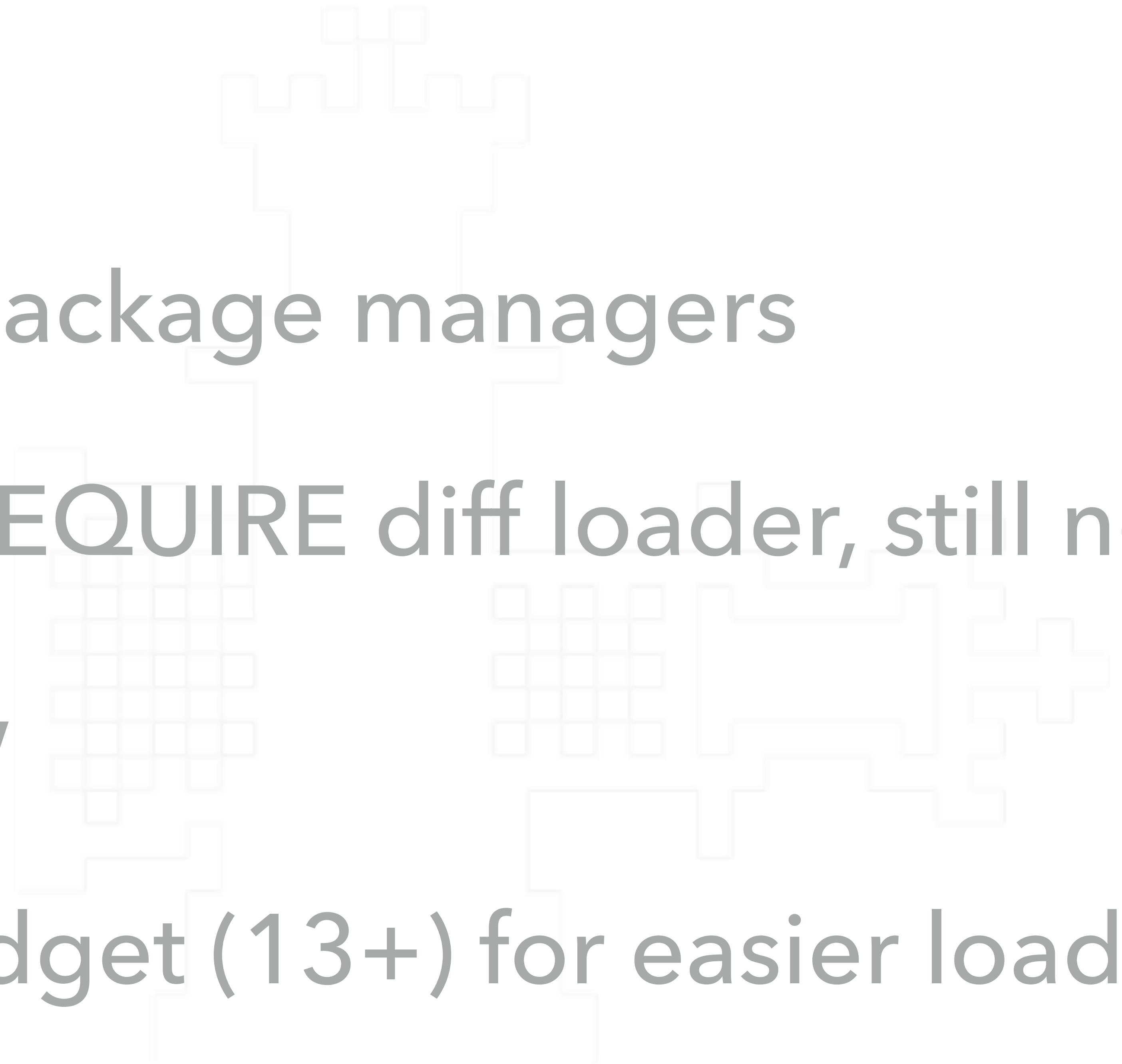
TVOS CHALLENGES

- 'sysstatuscheck' is missing from tvOS, causing crashes
- strict architecture checks causing more baffling launchd crashes
- framebuffer (sic) size, screen size would truncate the text
- no serial / JTAG debugging available (for 4th gen)
- no HDMI monitor (yet!) was filming output from the tv!

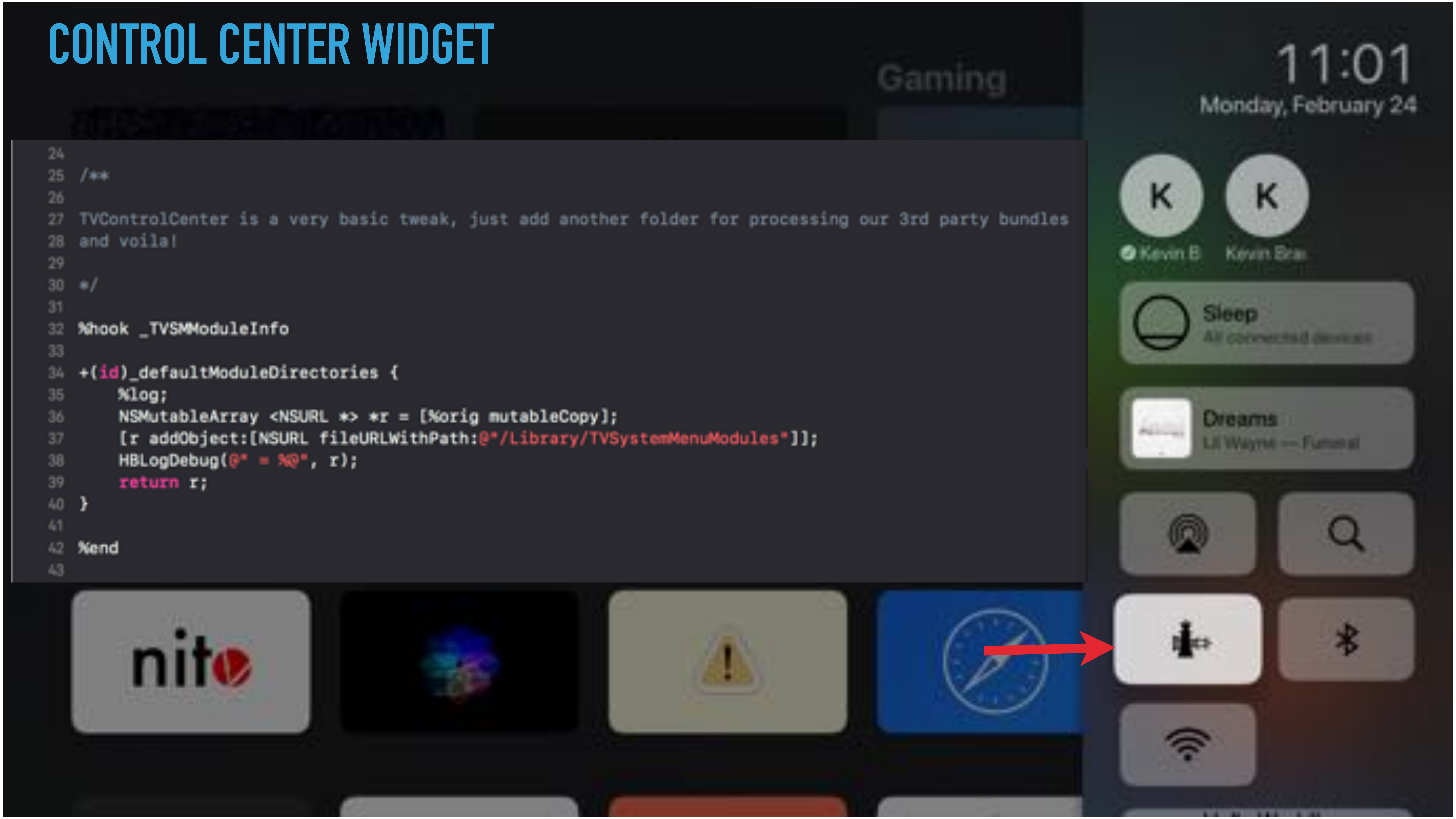
EARLY DEBUGGING – POST TV...

TVOS CHALLENGES CONTINUED

- tvOS specific loader creation
  - no need to select multiple package managers
  - different payload (doesn't REQUIRE diff loader, still notable)
  - unique post installation flow
  - includes a control center widget (13+) for easier loader access
  - no icons on home screen without code injection (uicache deficiency)
  - iOS / tvOS always require separate build at very least



CONTROL CENTER WIDGET



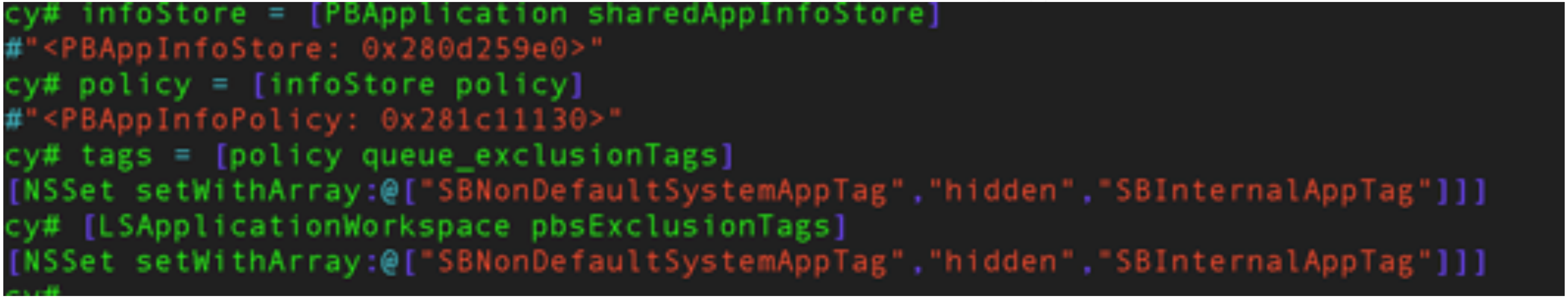
```
/**

TVControlCenter is a very basic tweak, just add another folder for processing our 3rd party bundles
and voila!

*/

%hook _TVSMModuleInfo

+(id)_defaultModuleDirectories {
    %log;
    NSMutableArray <NSURL *> *r = [%orig mutableCopy];
    [r addObject:[NSURL fileURLWithPath:@"/Library/TVSystemMenuModules"]];
    HBLogDebug(@" = %@", r);
    return r;
}

%end
```

CONTROL CENTER WIDGET IMPLEMENTATION

```
@implementation CRModule

+(long long)buttonStyle {
    return TVSMActionButtonStyleMedium;
}

-(id)contentViewController {

    TVSMButtonViewController *buttonController = (TVSMButtonViewController*)[super
        contentViewController];
    [buttonController setStyle:TVSMActionButtonStyleMedium];
    NSString *packageFile = [[self bundle] pathForResource:@"checkra1n" ofType:@"png"];
    //important to make this a template image so it works properly with both light and dark mode
    UIImage *theImage = [[UIImage imageWithContentsOfFile:packageFile]
        imageWithRenderingMode:UIImageRenderingModeAlwaysTemplate];
    [buttonController setImage:theImage];
    return buttonController;
}

-(void)handleAction {

    [[LSApplicationWorkspace defaultWorkspace] openApplicationWithBundleID:@"kjc.loader"];

}

-(BOOL)dismissAfterAction {
    return TRUE;
```

TVOS LOADER DIFFERENCES

- tvOS loader flavor installed with SBAppTags key: 'hidden'
- Allows loading application without additional checks visible apps undergo



```
cy# infoStore = [PBApplication sharedAppInfoStore]
#"<PBAppInfoStore: 0x280d259e0>"
cy# policy = [infoStore policy]
#"<PBAppInfoPolicy: 0x281c11130>"
cy# tags = [policy queue_exclusionTags]
[NSSet setWithArray:@["SBNonDefaultSystemAppTag","hidden","SBInternalAppTag"]]]
cy# [LSApplicationWorkspace pbsExclusionTags]
[NSSet setWithArray:@["SBNonDefaultSystemAppTag","hidden","SBInternalAppTag"]]]
cy#
```

checkra1n RC1.1 installer

** sandnand gang presents checkra1n for your apple television **

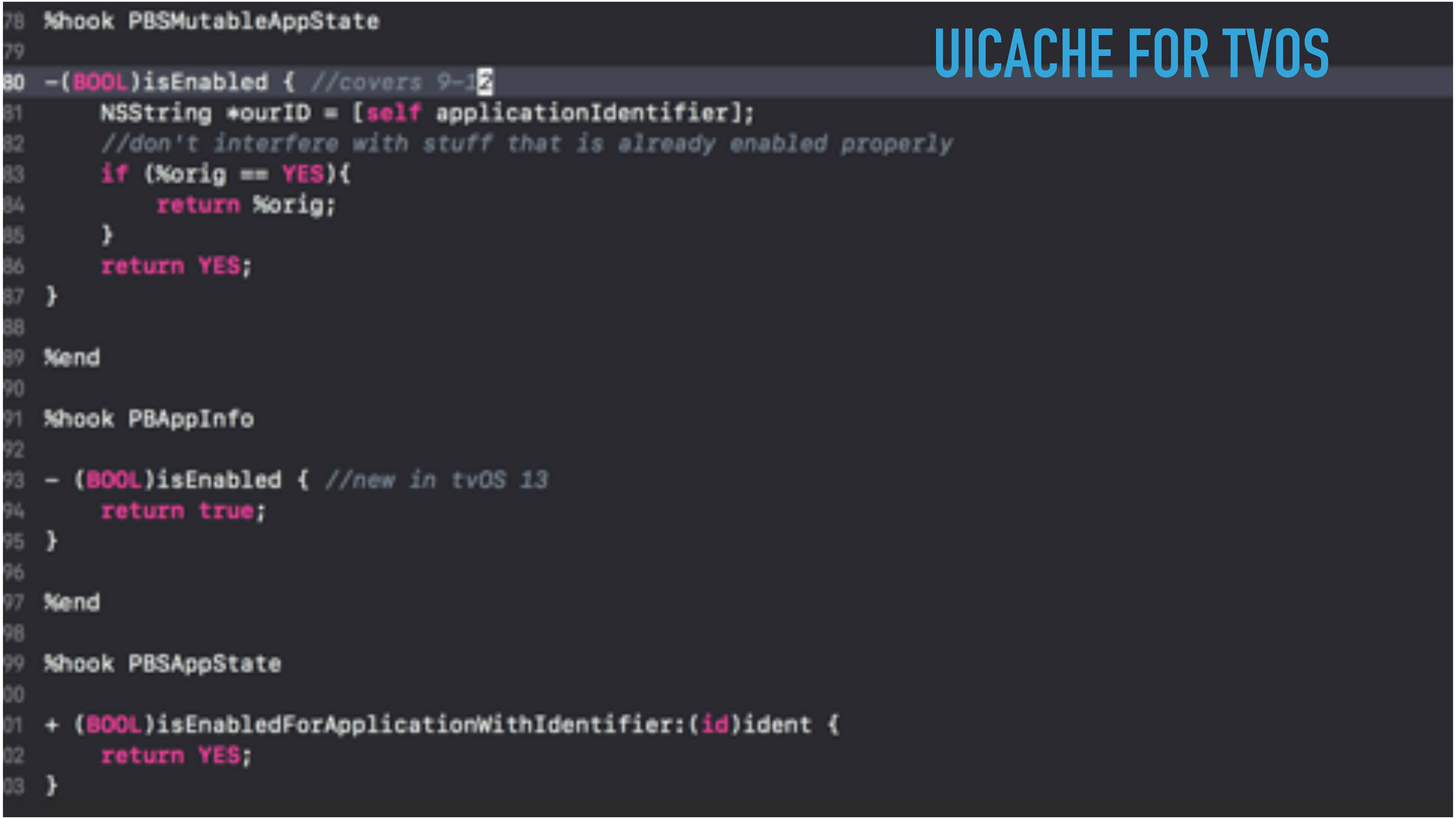
AppleTV6,2 named checkusb

Darwin Kernel Version 18.5.0: Wed Mar 13 15:19:12 PDT 2019; root:xnu-4903.253.2~6/RELEASE_ARM64_T8011

TVOS CHALLENGES CONTINUED

- tvOS uicache obstacles
  - (still) requires code injection
  - app loading changed in 13.x

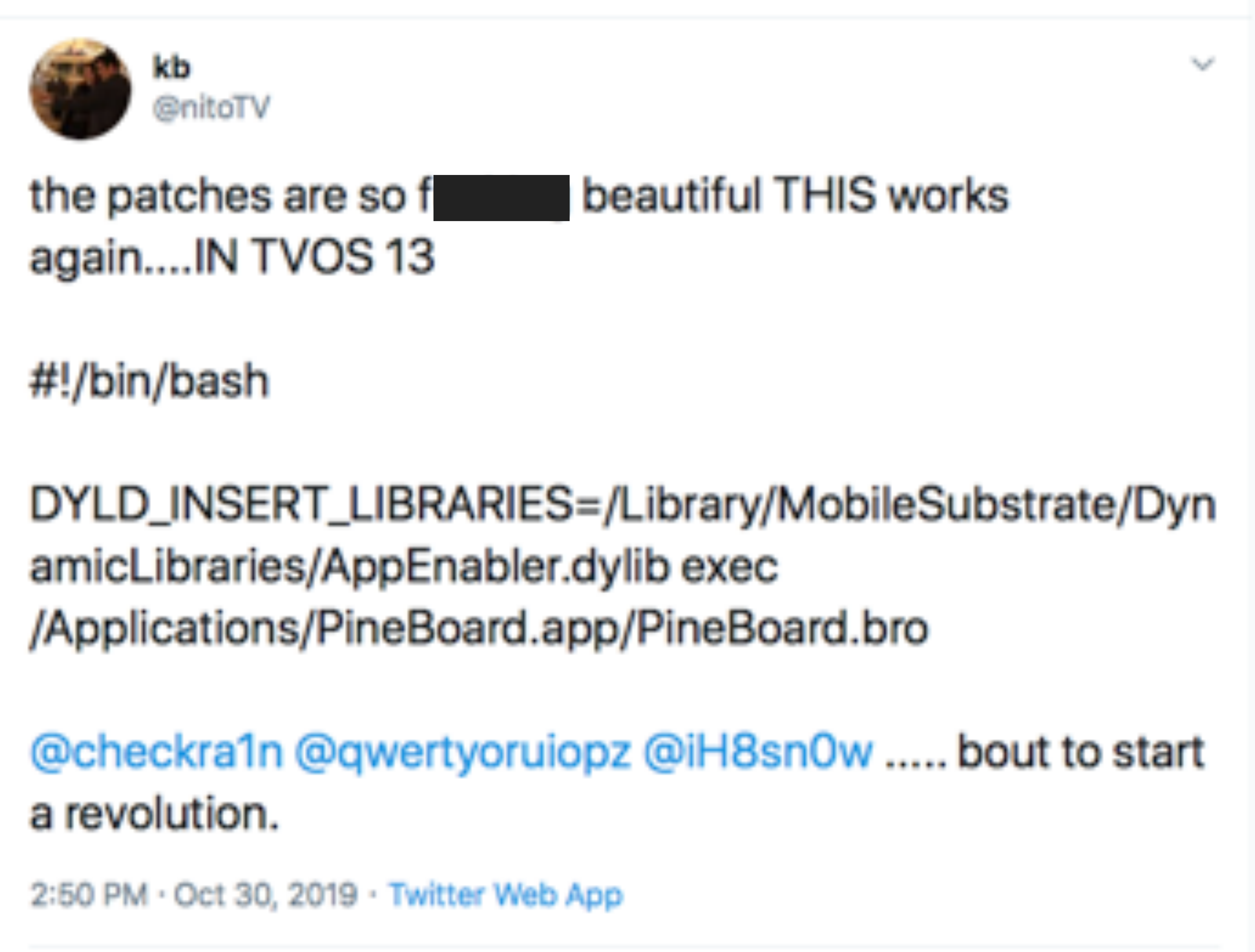
UICACHE FOR TVOS



```
%hook PBSMutableAppState

-(BOOL)isEnabled { //covers 9-12
    NSString *ourID = [self applicationIdentifier];
    //don't interfere with stuff that is already enabled properly
    if (%orig == YES){
        return %orig;
    }
    return YES;
}

%end

%hook PBAppInfo

- (BOOL)isEnabled { //new in tvOS 13
    return true;
}

%end

%hook PBSAppState

+ (BOOL)isEnabledForApplicationWithIdentifier:(id)ident {
    return YES;
}
```

TVOS CHALLENGES CONTINUED

- 13+ no easy code injection in early stages, used bootstrapping w/ substitute



kb
@nitoTV

the patches are so f[redacted] beautiful THIS works again....IN TVOS 13

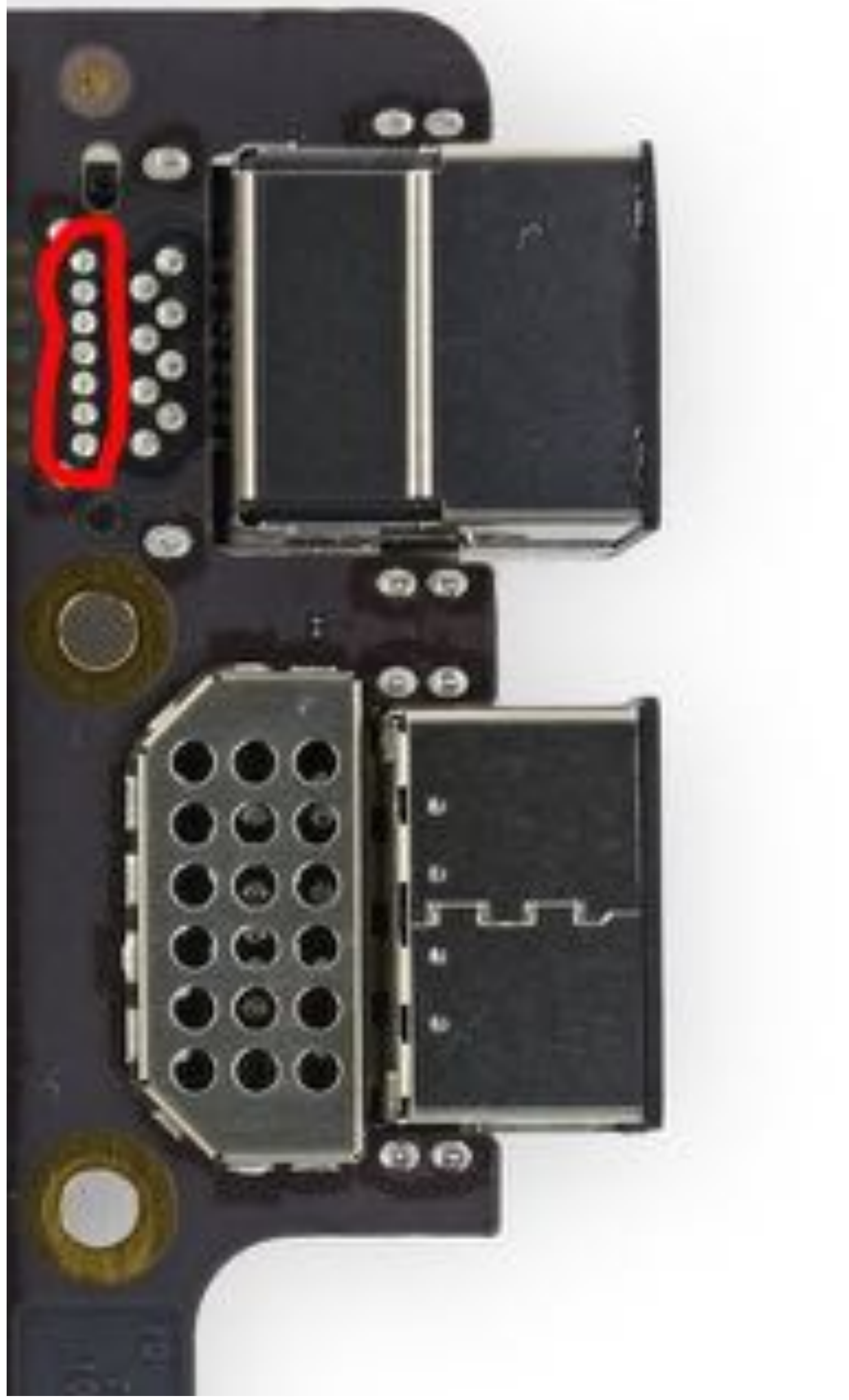
```
#!/bin/bash

DYLD_INSERT_LIBRARIES=/Library/MobileSubstrate/DynamicLibraries/AppEnabler.dylib exec /Applications/PineBoard.app/PineBoard.bro
```

@checkra1n @qwertyoruiopz @iH8sn0w ..... bout to start a revolution.

2:50 PM · Oct 30, 2019 · Twitter Web App

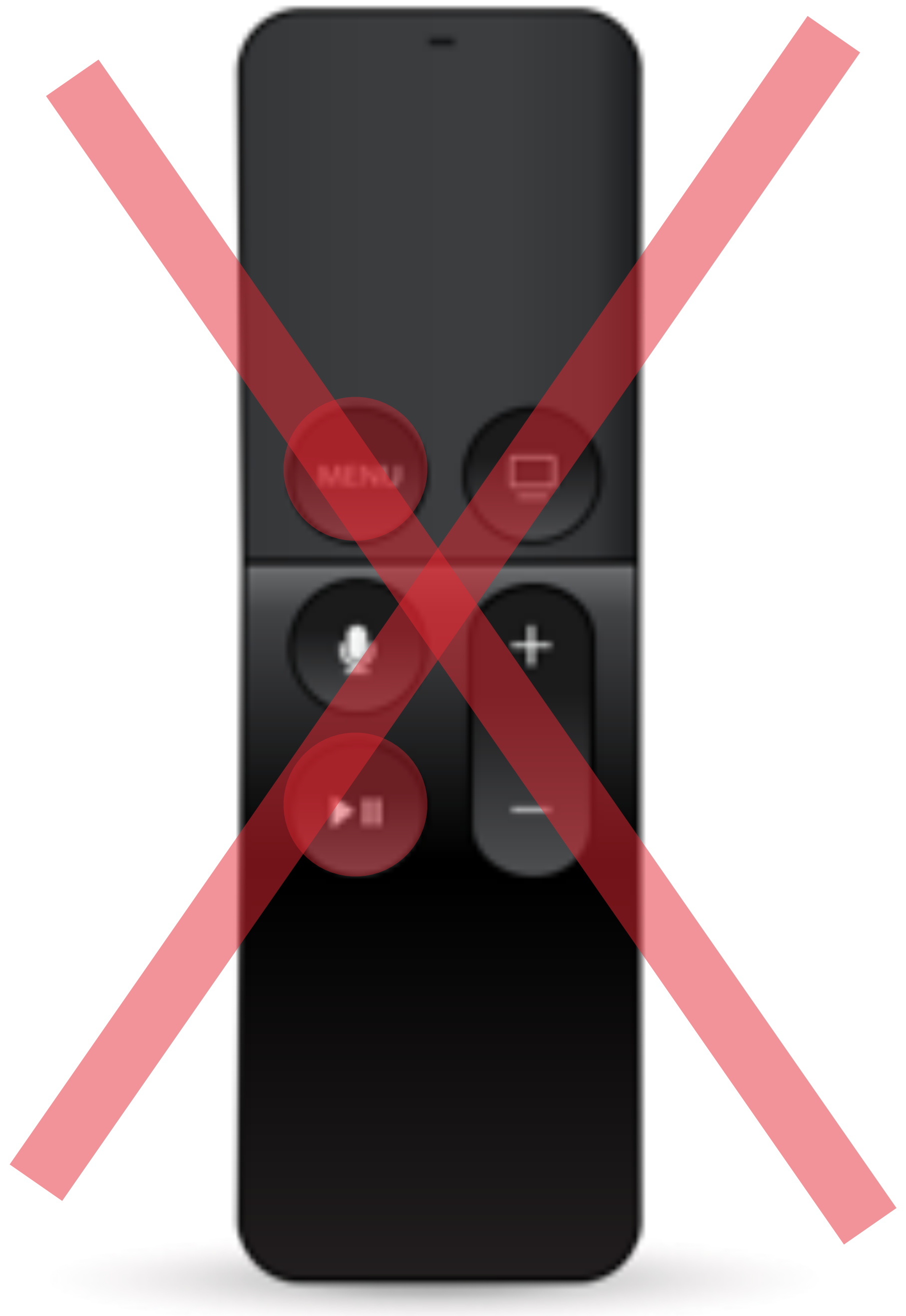
TVOS CHALLENGES CONTINUED

- 10.16.19 - checkra1n works on AppleTV 4
- 10.17.19 - Tease special pins on the 4K
- 10.22.19 - first successful "diags" on the 4K
- iBoot output, no serial yet
- 10.30.19 - First code injection achieved on tvOS 13

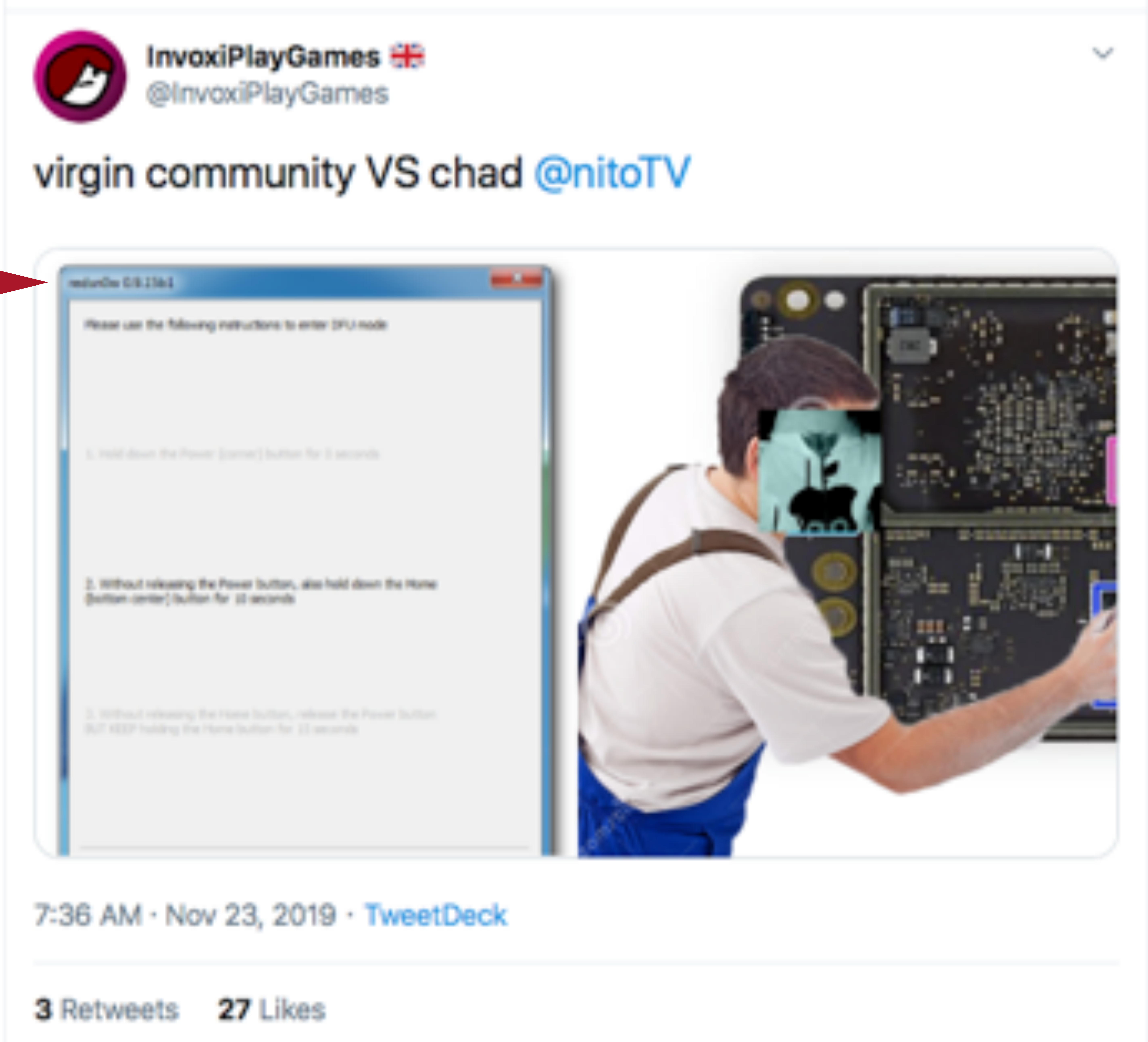


TVOS CHALLENGES CONTINUED

- 10.24.19 - Alleged sand NAND incident supposedly occurs
  - Goal is DFU, Menu+Play/Pause not working
  - Verify [redacted] can see device in Recovery mode on 4K
  - Bootloop achieved + [redacted] verifies DFU mode works



redsn0w 0.9.15b1



InvoxiPlayGames 🇬🇧
@InvoxiPlayGames

virgin community VS chad @nitoTV

redsn0w 0.9.15b1

Please use the following instructions to enter DFU mode

1. Hold down the Power (corner) button for 3 seconds

2. Without releasing the Power button, also hold down the Home (bottom center) button for 10 seconds

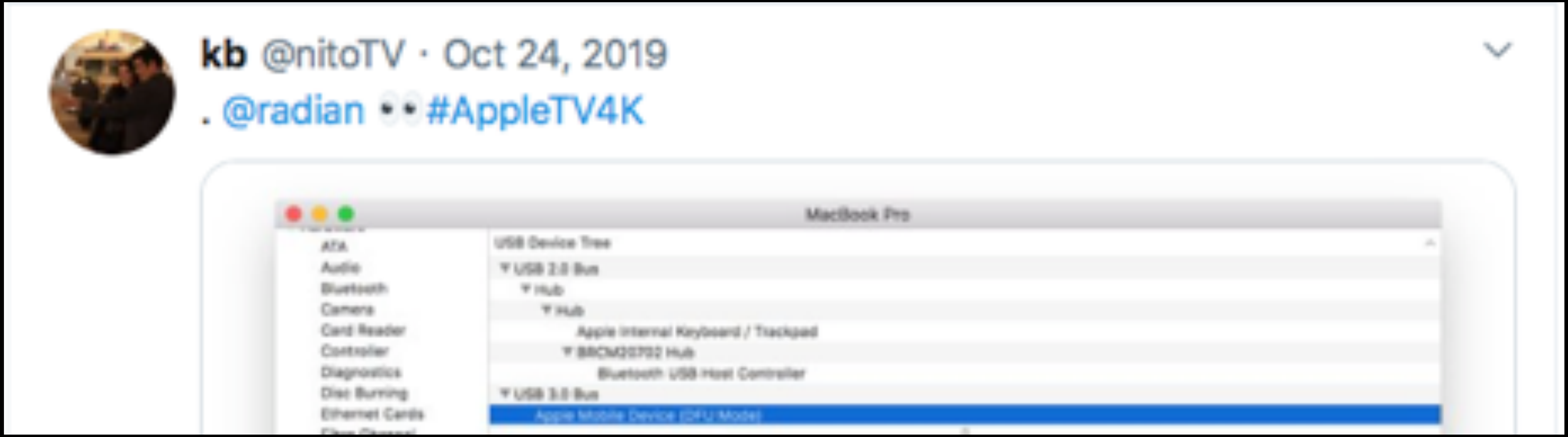
3. Without releasing the Home button, release the Power button BUT KEEP holding the Home button for 15 seconds

7:36 AM · Nov 23, 2019 · TweetDeck

3 Retweets 27 Likes

#sandnandgang

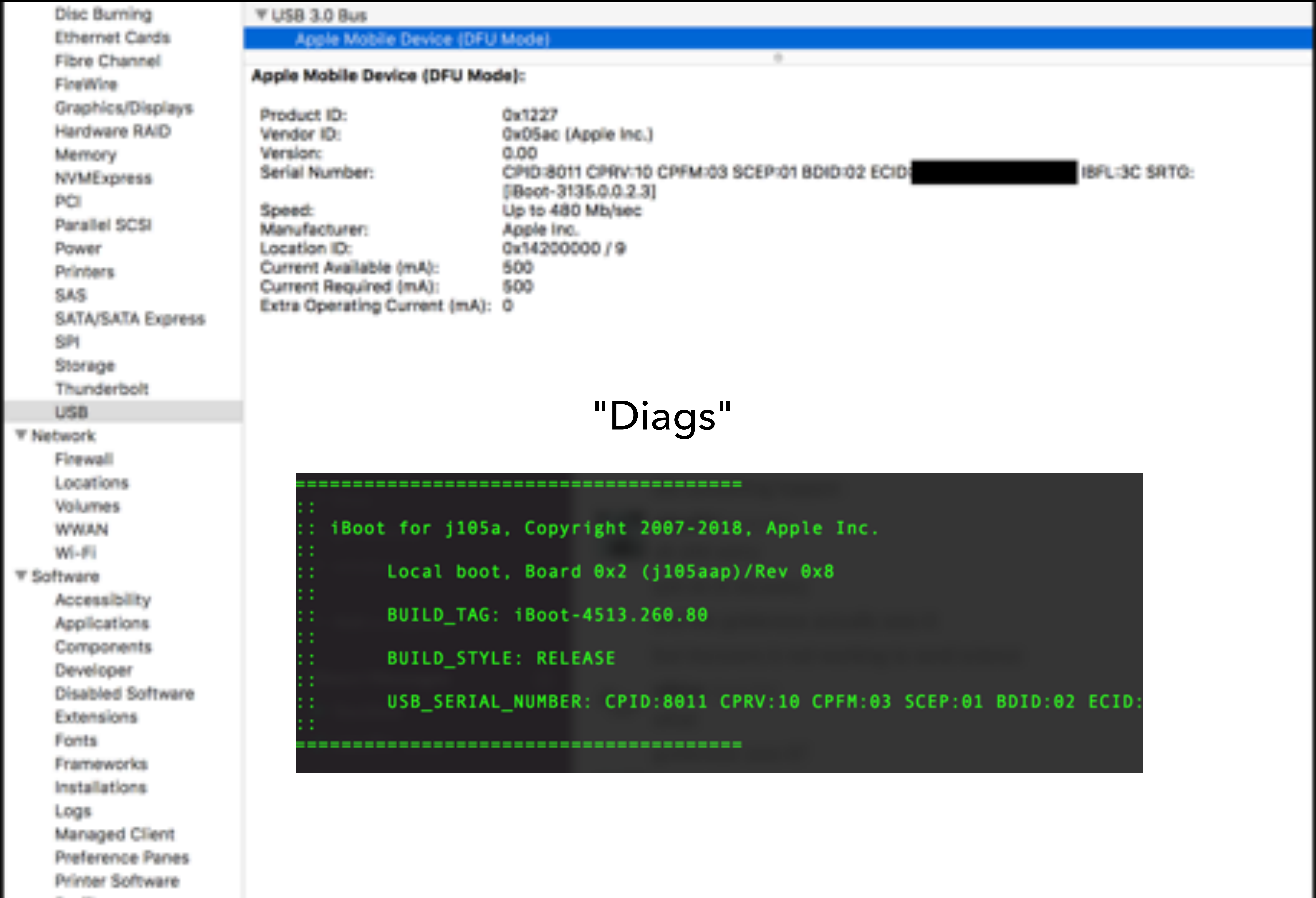
HAVE A LITTLE FUN W/ @RADIAN ON TWITTER



kb @nitoTV · Oct 24, 2019

. @radian 👀 #AppleTV4K

```
USB Device Tree
▼ USB 2.0 Bus
  ▼ Hub
    ▼ Hub
        Apple Internal Keyboard / Trackpad
      ▼ BRCM20702 Hub
          Bluetooth USB Host Controller
▼ USB 3.0 Bus
    Apple Mobile Device (DFU Mode)
```

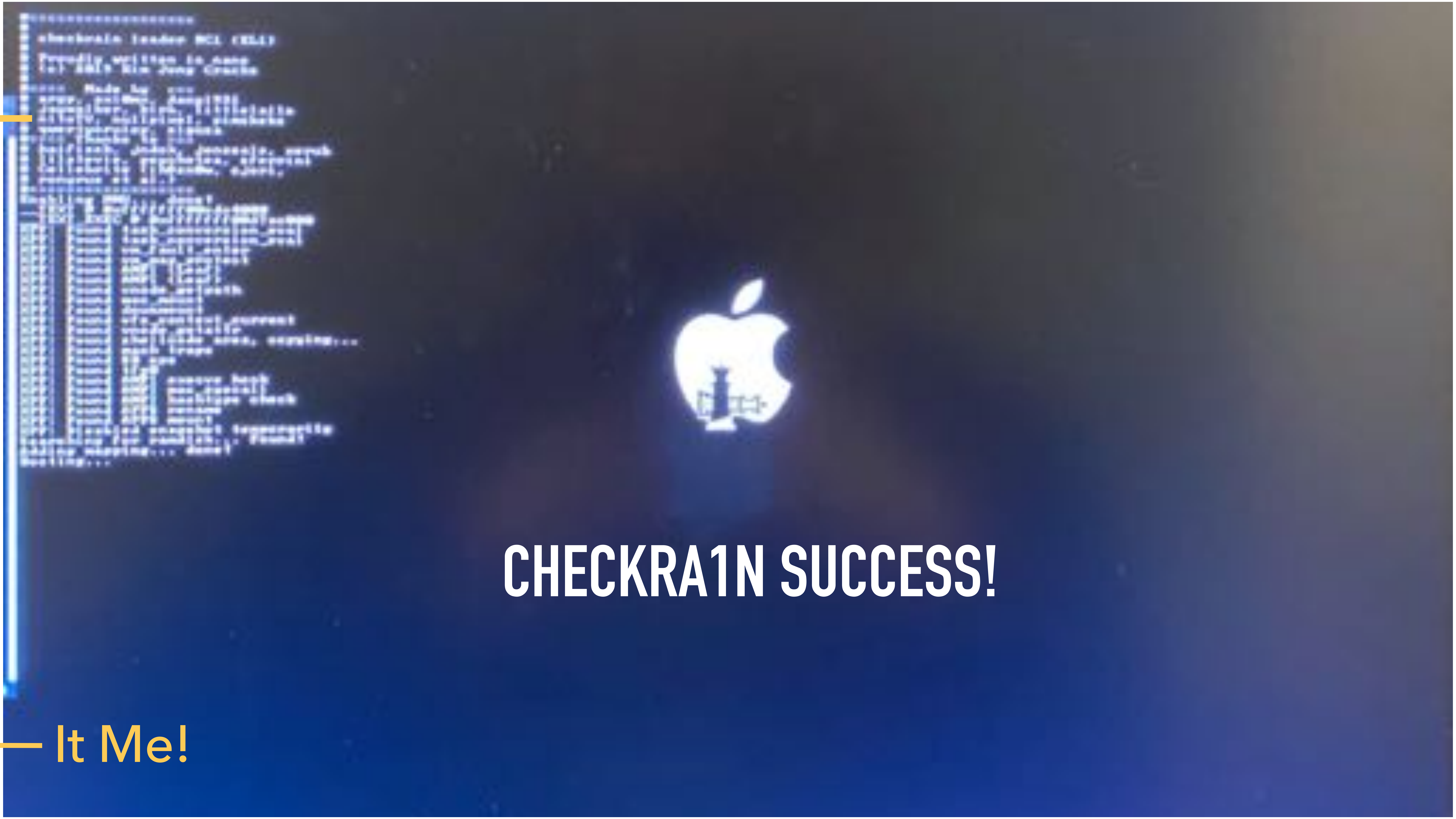


Apple Mobile Device (DFU Mode):

```
Product ID:                    0x1227
Vendor ID:                     0x05ac (Apple Inc.)
Version:                       0.00
Serial Number:                 CPID:8011 CPRV:10 CPFM:03 SCEP:01 BDID:02 ECID:[redacted] IBFL:3C SRTG:
                               [iBoot-3135.0.0.2.3]
Speed:                         Up to 480 Mb/sec
Manufacturer:                  Apple Inc.
Location ID:                   0x14200000 / 9
Current Available (mA):        500
Current Required (mA):         500
Extra Operating Current (mA):  0
```

"Diags"

```
=======================================
::
:: iBoot for j105a, Copyright 2007-2018, Apple Inc.
::
::      Local boot, Board 0x2 (j105aap)/Rev 0x8
::
::      BUILD_TAG: iBoot-4513.260.80
::
::      BUILD_STYLE: RELEASE
::
::      USB_SERIAL_NUMBER: CPID:8011 CPRV:10 CPFM:03 SCEP:01 BDID:02 ECID:
::
=======================================
```



```
checkra1n loader [illegible]
Proudly written in nano
(c) 2019 Kim Jong Cracks
==== Made by ====
[illegible]
[illegible]
[illegible] Found [illegible] shellcode area, copying...
[illegible]
Adding mapping... done!
Booting...
```

CHECKRA1N SUCCESS!

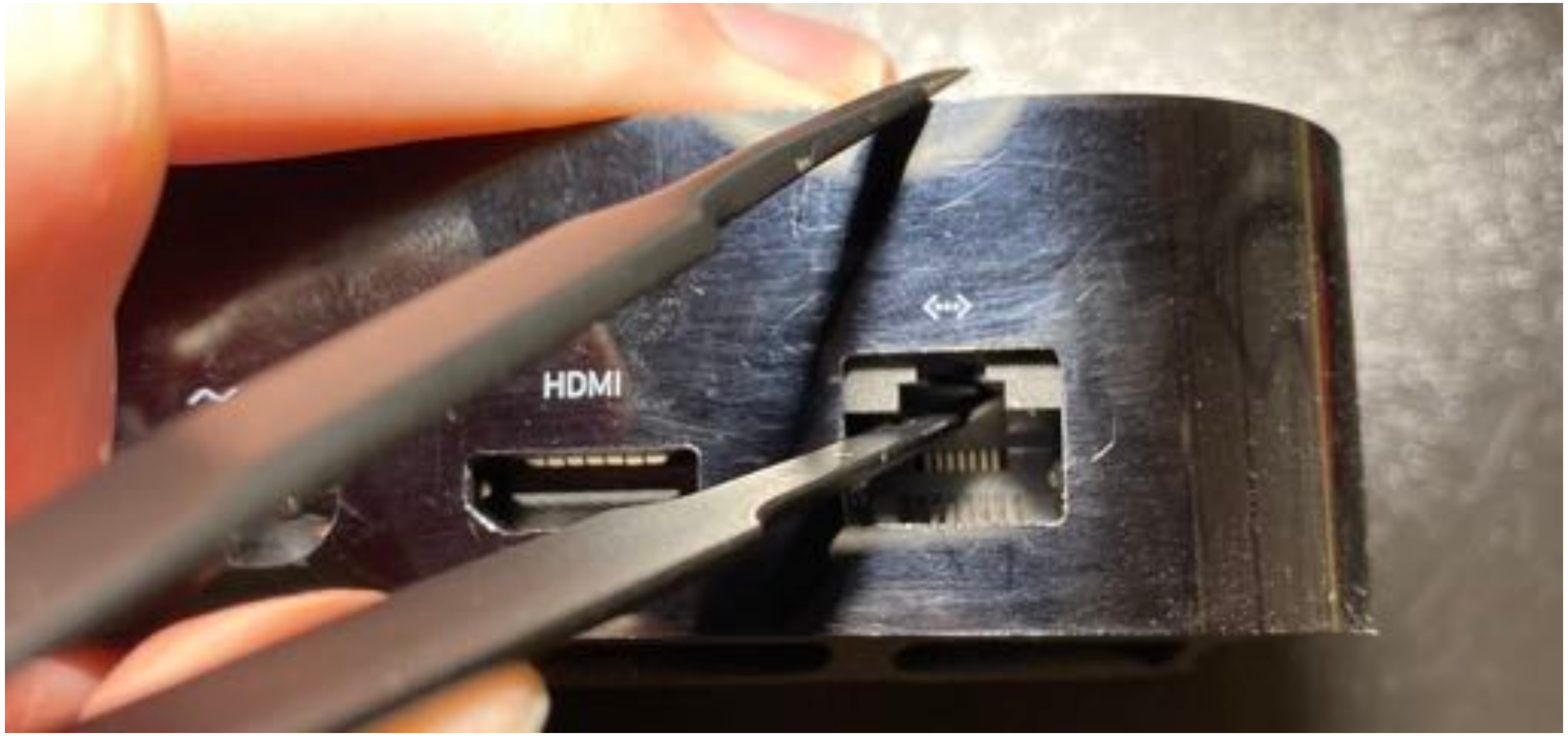
It Me!

CHECKRA1N 4K EDITION..WITH HELP!

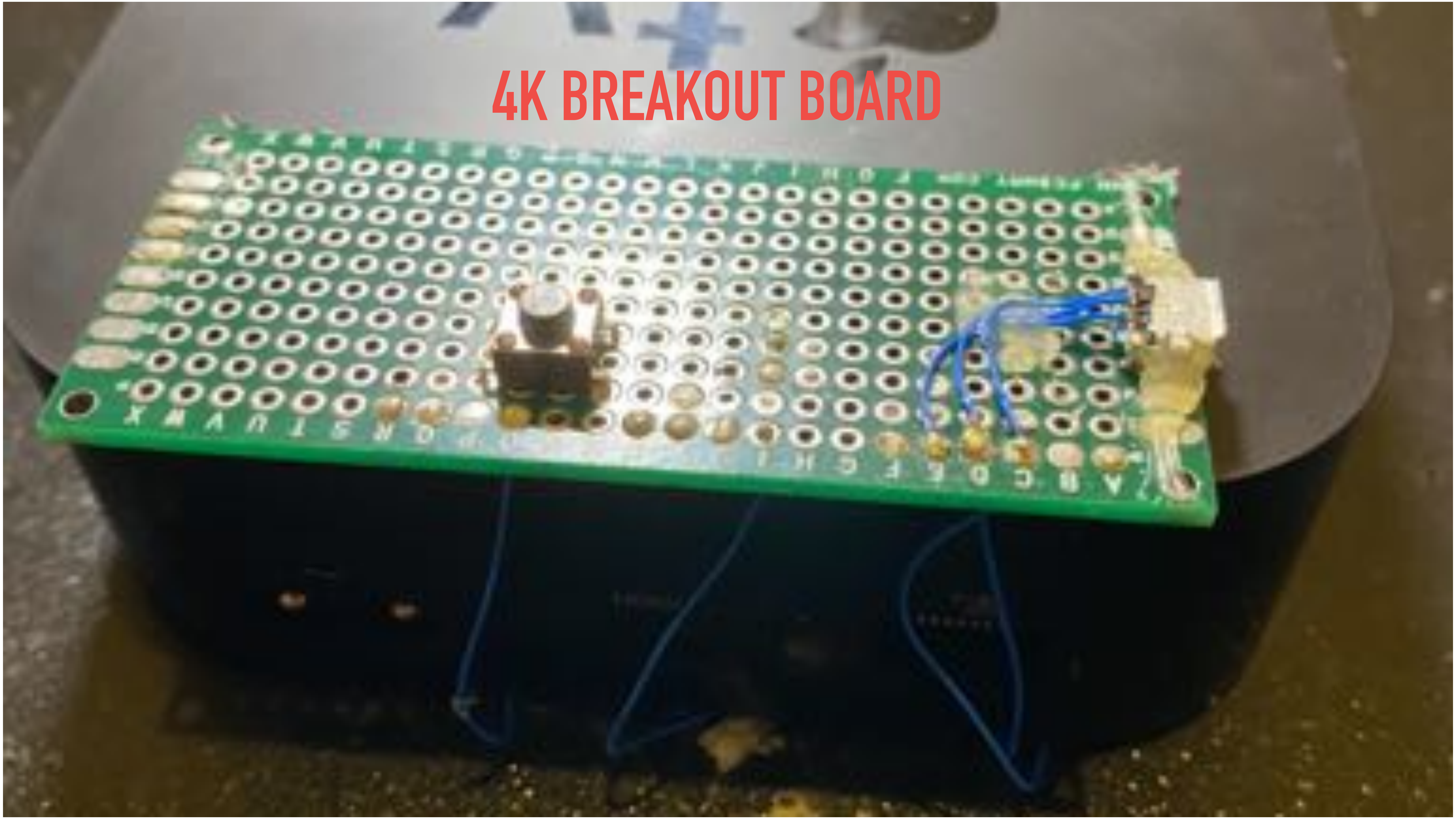
@LITTLESTEVE OF GUARDIAN

TVOS 4K CHALLENGES

- 11.8.19 - @littlesteve achieves DFU + first checkra1n tvOS 4K jailbreak
- 11.17.19 @littlesteve spills the beans on the ethernet trapdoor on the 4K



4K BREAKOUT BOARD



4K BEDLAM

- USB Wired and working without [redacted] but suffers same failure to enter DFU.
- First forced DFU entry perfect for experimentation, illegitimate for tvOS boots.
- Third time's a charm. Holding PCIe reset on NVMe enters usable DFU with no side effects.
- Discovered debug serial port on testpoints.
- Further hardware exploration a topic for another day
- Keep your eyes on guardianapp.com for more!

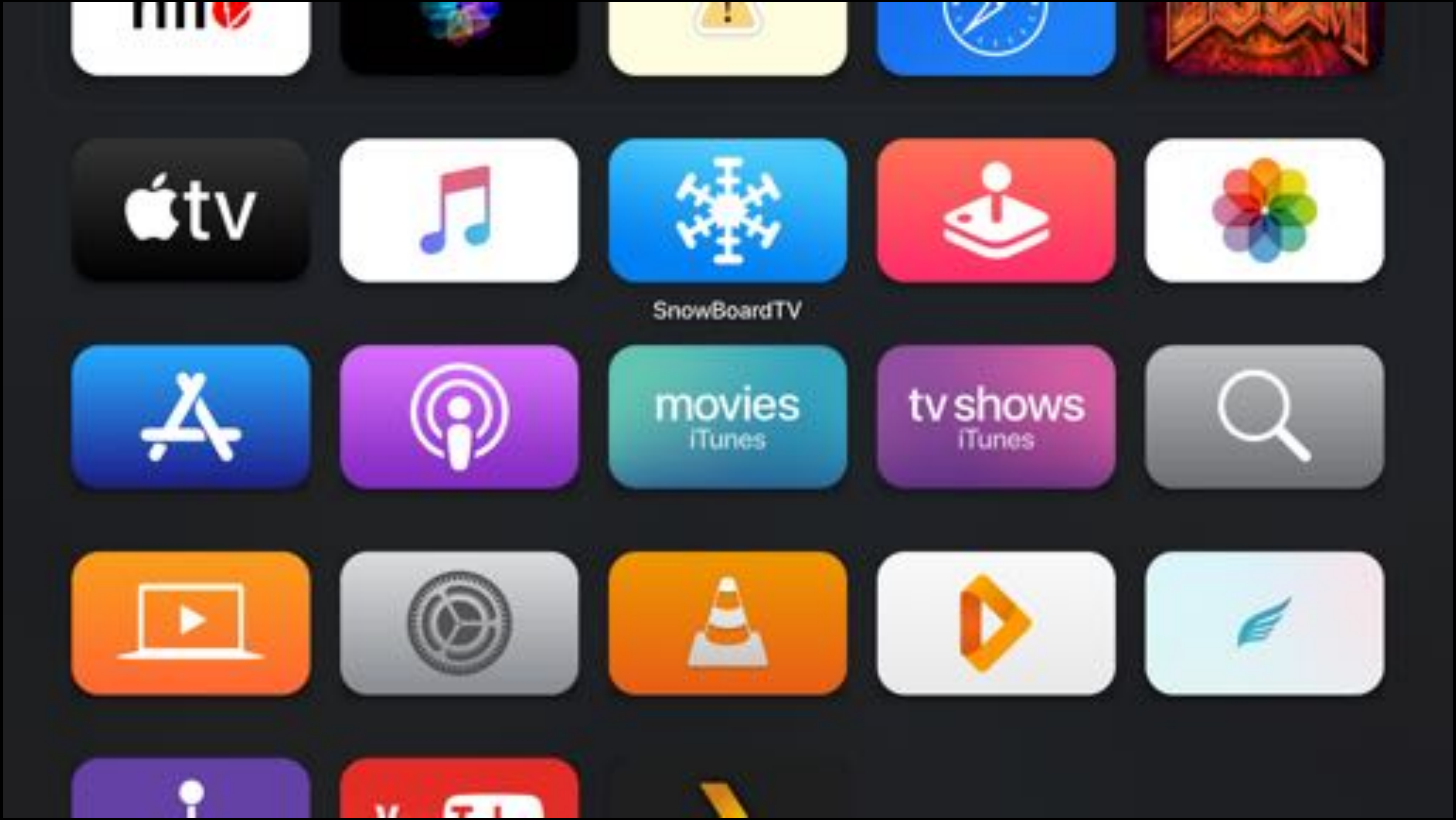
AFTERMATH

- Consumed with tvOS 13 support, so many new things!!
- Grappled with substitute / substrate issues between both jailbreaks (chimera/ checkra1n)
  - "Forces" repository split for checkra1n / tvOS in nitoTV
  - No 'proper' way for code injection with substitute in checkra1n / tvOS 13
- Started work on migrating away from maintaining apt/dpkg for Elucubratus

AFTERMATH

- @sparkdev_ & @iKilledAppl3 make a huge splash
- SnowBoard TV (theming on tvOS! first ever!)
- AirDrop updates & improvements - feature parity with iOS & tvOS
- Update nitoTV + Breezy + ReProvisionTV, Ethereal etc..
- Planning on free tvOS development class in 2020
- HarlemShakeTV only a demo can explain!

DOOM
12:07
Monday, February 24
K
Kevin B
K
Kevin Bra
Sleep
All connected devices
Not Playing
nito


tv
SnowBoardTV
movies
iTunes
tv shows
iTunes

THANK YOU!

Resources: tvOS Blog Post https://sciencography.tumblr.com/post/187244563802/growup

https://github.com/Lechium

https://git.nito.tv

Kevin.Bradley@guardianapp.com

QUESTIONS??